CLAIMS

What is claimed is:

1. A computer-implemented method of operating a reference monitor simulator operable to recreate the operations performed by a reference monitor on a computer system, the method comprising:

(A) defining at least one security rule specifying whether to allow or deny a request to access at least one resource under a given set of circumstances;

(B) supplying at least one request to access a resource; and

(C) applying the at least one security rule in response to the at least one request to access a resource to determine whether to allow or prevent the at least one request.

2. The method of claim 1, further comprising providing at least one parameter defining the system environment in which the reference monitor executes.

3. The method of claim 2, wherein the at least one parameter includes a time parameter which defines the passage of time perceived by the computer system.

4. The method of claim 3, wherein the passage of time indicated by the time parameter is faster than the actual passage of time.

5. The method of claim 4, wherein the passage of time indicated by the time parameter enables the computer system to execute the reference monitor simulator in an accelerated manner.

6. The method of claim 1, further comprising:

(D) assessing the effectiveness of the at least one security rule.

7. The method of claim 6, wherein assessing the effectiveness of the security rule further comprises determining at least one of the number of improper access requests prevented and the number of proper access requests allowed.

8. The method of claim 6, wherein assessing the effectiveness of the security rule further comprises determining a rate of improper requests prevented.

9. The method of claim 1, wherein (B) further comprises an application program supplying the at least one request to access a resource.

10. The method of claim 1, wherein (B) further comprises capturing at least one request to access a resource before supplying the at least one request to access a resource.

11. The method of claim 10, wherein a reference monitor performs the capture of the at least one request to access a resource.

12. The method of claim 11, wherein the reference monitor which performs the capture of the at least one request to access a resource is the same type of reference monitor as the reference monitor whose operations are recreated by the reference monitor simulator.

13. The method of claim 10, wherein the captured at least one request to access a resource is an improper request.

14. The method of claim 13, wherein an improper request comprises a request issued by an application in response to one of a virus and a buffer overrun attack.

15. The method of claim 10, wherein the captured at least one request is modified prior to supplying the at least one request to access a resource.

16. The method of claim 15, wherein the modification is performed by a user.

17. The method of claim 6, wherein an electronic file system stores the at least one security rule, and wherein (D) further comprises the reference monitor simulator accessing the security rule in the electronic file system in response to receiving the at least one request to access a resource.

18. The method of claim 2, wherein the at least one parameter provided to the reference monitor simulator further includes at least one of a system clock, a wrapper function, and a timer event.

19. The method of claim 1, further comprising:

(E) maintaining statistics on the operation of the reference monitor simulator.

20. The method of claim 19, wherein the statistics include at least one of the number of requests per resource, number of total requests, type of request per resource, total of each type of request, number of queries, number of callbacks, number of requests allowed compared to number of requests expected, and number of requests prevented compared to number of prevented requests expected.

21. A computer-readable medium having instructions recorded thereon which, when executed by a computer, cause the computer to perform a method of operating a reference monitor simulator operable to recreate the operations performed by a reference monitor on a computer system, the method comprising:

(A) defining at least one security rule specifying whether to allow or deny a request to access at least one resource under a given set of circumstances;

(B) supplying at least one request to access a resource; and

(C) applying the at least one security rule in response to the at least one request to access a resource to determine whether to allow or prevent the at least one request.

22. The computer-readable medium of claim 21, further comprising instructions defining providing at least one parameter defining the system environment in which the reference monitor executes.

23. The computer-readable medium of claim 22, wherein the at least one parameter includes a time parameter which defines the passage of time perceived by the computer system.

24. The computer-readable medium of claim 23, wherein the passage of time indicated by the time parameter is faster than the actual passage of time.

25. The computer-readable medium of claim 24, wherein the passage of time indicated by the time parameter enables the computer system to execute the reference monitor simulator in an accelerated manner.

26. The computer-readable medium of claim 21, further comprising instructions defining:

(D) assessing the effectiveness of the at least one security rule.

27. The computer-readable medium of claim 26, wherein assessing the effectiveness of the security rule comprises determining at least one of the number of improper access requests prevented and the number of proper access requests allowed.

28. The computer-readable medium of claim 26, wherein assessing the effectiveness of the security rule comprises determining a rate of improper requests prevented.

29. The computer-readable medium of claim 21, wherein (B) further comprises an application program supplying the at least one request to access a resource.

30. The computer-readable medium of claim 21, wherein (B) further comprises capturing at least one request to access a resource before supplying the at least one request to access a resource.

31. The computer-readable medium of claim 30, further comprising instructions defining a reference monitor performing the capture of the at least one request to access a resource.

32. The computer-readable medium of claim 31, wherein the reference monitor which performs the capture of the at least one request to access a resource is the same type of reference monitor as the reference monitor whose operations are recreated by the reference monitor simulator.

33. The computer-readable medium of claim 30, wherein the captured at least one request to access a resource is an improper request.

34. The computer-readable medium of claim 33, wherein an improper request comprises a request issued by an application in response to one of a virus and a buffer overrun attack.

35. The computer-readable medium of claim 30, wherein the captured at least one request is modified prior to supplying the at least one request to access a resource.

36. The computer-readable medium of claim 35, wherein the modification is performed by a user.

37. The computer-readable medium of claim 26, further comprising instructions defining an electronic file system storing the at least one security rule, and wherein (D) further comprises the reference monitor simulator accessing the security rule in the electronic file system in response to receiving the at least one request to access a resource.

38. The computer-readable medium of claim 22, wherein the at least one parameter provided to the reference monitor simulator further includes at least one of a system clock, a wrapper function, and a timer event.

39. The computer-readable medium of claim 21, further comprising instructions defining:

(E) maintaining statistics on the operation of the reference monitor simulator.

40. The computer-readable medium of claim 39, wherein the statistics include at least one of the number of requests per resource, number of total requests, type of request per resource, total of each type of request, number of queries, number of callbacks, number of requests allowed compared to number of requests expected, and number of requests prevented compared to number of prevented requests expected.

41. A system for providing a reference monitor simulator for simulating the operations performed by a reference monitor, the system comprising:

a definer component to define at least one security rule specifying whether to allow or deny a request to access at least one resource under a given set of circumstances;

a supplier component to supply at least one request to access a resource; and

an applier component to apply the at least one security rule in response to the at least one request to access a resource to determine whether to allow or prevent the at least one request.

42. The system of claim 41, further comprising a provider component to provide at least one parameter defining the system environment in which the reference monitor executes.

43. The system of claim 42, wherein the at least one parameter includes a time parameter which defines the passage of time perceived by the computer system.

44. The system of claim 43, wherein the passage of time indicated by the time parameter is faster than the actual passage of time.

45. The system of claim 44, wherein the passage of time indicated by the time parameter enables the system to execute the reference monitor simulator in an accelerated manner.

46. The system of claim 41, further comprising an assessor component to assess the effectiveness of the at least one security rule.

47. The system of claim 46, wherein assessing the effectiveness of the security rule further comprises determining at least one of the number of improper access requests prevented and the number of proper access requests allowed.

48. The system of claim 46, wherein assessing the effectiveness of the security rule further comprises determining a rate of improper requests prevented.

49. The system of claim 41, further comprising an application program to supply the supplier component with the at least one request to access a resource.

50. The system of claim 41, further comprising a capture component to capture at least one request to access a resource before supplying the at least one request to access a resource.

51. The system of claim 50, wherein the capture component includes a second reference monitor.

52. The system of claim 51, wherein the second reference monitor is a same type of reference monitor as the reference monitor whose operations are recreated by the reference monitor simulator.

53. The system of claim 50, wherein the capture component captures at least one request to access a resource which is an improper request.

54. The system of claim 53, wherein an improper request comprises a request issued by an application in response to one of a virus and a buffer overrun attack.

55. The system of claim 50, further comprising a modification component to modify at least one captured request prior to supplying the at least one request to access a resource.

56. The system of claim 55, wherein the modification component takes input from a user.

57. The system of claim 41, further comprising an electronic file system which stores the at least one security rule, and the applier component accesses the security rule in the electronic file system in response to receiving at least one request to access a resource.

58. The system of claim 42, wherein the provider component provides at least one parameter to the reference monitor simulator which includes at least one of a system clock, a wrapper function, and a timer event.

59. The system of claim 41, further comprising:

(E) a statistics component to maintain statistics on the operation of the reference monitor simulator.

60. The system of claim 59, wherein the statistics component maintains statistics which include at least one of the number of requests per resource, number of total requests, type of request per resource, total of each type of request, number of queries, number of callbacks, number of requests allowed compared to number of requests expected, and number of requests prevented compared to number of prevented requests expected.

61. A signal embodied in a transmission medium, the signal operable to provide a reference monitor simulator to recreate the operations performed by a first reference monitor on a computer system, the signal comprising:

a first segment including a security rule specifying whether to allow or deny a request to access a resource under a given set of circumstances;

a second segment including a request to access a resource; and

a third segment including instructions to apply the at least one security rule in response to the request to determine whether to allow or prevent the at least one request.

62. The signal of claim 61, further comprising a parameter defining the computer system environment.

63. The signal of claim 62, wherein the parameter includes a time parameter which defines the passage of time perceived by the computer system.

64. The signal of claim 63, wherein the passage of time indicated by the time parameter is faster than the actual passage of time.

65. The signal of claim 64, wherein the passage of time indicated by the time parameter enables the computer system to execute in an accelerated manner.

66. The signal of claim 61, further comprising instructions to assess the effectiveness of the security rule.

67. The signal of claim 66, wherein assessing the effectiveness of the security rule comprises determining at least one of the number of improper access requests prevented and the number of proper access requests allowed.

68. The signal of claim 66, wherein assessing the effectiveness of the security rule comprises determining a rate of improper requests prevented.

69. The signal of claim 61, further comprising a request to access a resource.

70. The signal of claim 69, wherein the request is issued by an application program.

71. The signal of claim 69, wherein the request is captured by a second reference monitor.

72. The signal of claim 71, wherein the second reference monitor is a same type of reference monitor as the first reference monitor whose operations are recreated.

73. The signal of claim 71, wherein the request is an improper request.

74. The signal of claim 73, wherein an improper request comprises a request issued by an application program in response to one of a virus and a buffer overrun attack.

75. The signal of claim 69, wherein the request is modified prior to its being supplied.

76. The signal of claim 75, wherein the modification is performed by a user.

77. The signal of claim 61, wherein an electronic file system stores the at least one security rule, and wherein the signal further comprises instructions to access the security rule in the electronic file system in response to receiving the request to access a resource.

78. The signal of claim 62, further comprising a parameter including a system clock, a wrapper function, and a timer event.

79. The signal of claim 61, further comprising instructions to maintain statistics on the operation of the reference monitor simulator.

80. The signal of claim 79, wherein the statistics include at least one of the number of requests per resource, number of total requests, type of request per resource, total of each type of request, number of queries, number of callbacks, number of requests allowed compared to number of requests expected, and number of requests prevented compared to number of prevented requests expected.

81. A method of evaluating a security rule on a computer system, the method comprising:

(A) applying, by a reference monitor simulator operable to recreate operations performed by a first reference monitor, a security rule in response to receiving a request to access a resource, the security rule defining whether to allow or prevent the request;

(B) assessing the effectiveness of the security rule.

82. The method of claim 81, further comprising:

(C) providing at least one parameter defining the system environment in which the security rule is applied.

83. The method of claim 82, wherein the at least one parameter includes a time parameter which defines the passage of time perceived by the computer system.

84. The method of claim 83, wherein the passage of time indicated by the time parameter is faster than the actual passage of time.

85. The method of claim 84, wherein the passage of time indicated by the time parameter enables the reference monitor simulator to execute in an accelerated manner.

86. The method of claim 81, wherein assessing the effectiveness of the security rule includes determining at least one of the number of improper access requests prevented and the number of proper access requests allowed.

87. The method of claim 86, wherein assessing the effectiveness of the security rule includes determining a rate of improper requests prevented.

88. The method of claim 81, wherein (A) further comprises applying the security rule in response to receiving a request issued by an application program.

89. The method of claim 88, wherein the request is captured.

90. The method of claim 89, wherein the capture is performed by a second reference monitor.

91. The method of claim 90, wherein the second reference monitor is the same type of reference monitor as the first reference monitor whose operations are recreated by the reference monitor simulator.

92. The method of claim 89, wherein the captured request is an improper request.

93. The method of claim 92, wherein an improper request includes a request issued in response to one of a virus and a buffer overrun attack.

94. The method of claim 89, wherein the captured request is modified prior to applying the security rule.

95. The method of claim 94, wherein the modification is performed by a user.

96. The method of claim 82, wherein the at least one parameter includes at least one of a system clock, a wrapper function, and a timer event.

97. The method of claim 81, wherein (B) further comprises maintaining statistics on the application of the security rule.

98. The method of claim 97, wherein the statistics include at least one of the number of requests per resource, number of total requests, type of request per resource, total of each type of request, number of queries, number of callbacks, number of requests allowed compared to number of requests expected, and number of requests prevented compared to number of prevented requests expected.